



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/068,280	02/04/2002	Mark J. McArdle	01.239.01	9739
7590	03/15/2006		EXAMINER	
ZILKA-KOTAB PC PO Box 721120 San Jose, CA 95172-1120			HA, LEYNNA A	
			ART UNIT	PAPER NUMBER
			2135	

DATE MAILED: 03/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<p style="text-align: center;">Advisory Action Before the Filing of an Appeal Brief</p>	Application No.	Applicant(s)	
	10/068,280	MCARDLE ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

THE REPLY FILED 13 February 2006 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1 The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

a) The period for reply expires 3 months from the mailing date of the final rejection.

b) The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because

(a) They raise new issues that would require further consideration and/or search (see NOTE below);

(b) They raise the issue of new matter (see NOTE below);

(c) They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or

(d) They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. Applicant's reply has overcome the following rejection(s): _____.

6. Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. For purposes of appeal, the proposed amendment(s): a) will not be entered, or b) will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: _____

Claim(s) objected to: _____

Claim(s) rejected: 1-51

Claim(s) withdrawn from consideration: _____

AFFIDAVIT OR OTHER EVIDENCE

8. The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. The request for reconsideration has been considered but does NOT place the application in condition for allowance because:
See Continuation Sheet.

12. Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). _____

13. Other: _____

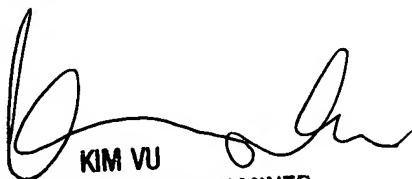
Continuation of 11. does NOT place the application in condition for allowance because: the examiner maintains the rejection in view of Freund and Kaler, et al.

The security system of Freund and performance analyzer of Kaler both monitors and filters data and therefore both comprises security prevention. A security system and a performance analyzer both analyzes and monitors the systems. To analyze the performance is clearly to attempt to protect the system, otherwise there is not a need to analyze its traffic or activities. Freund's invention monitors file activity (col.4, lines 64-67) and unsafe/unwanted traffic of the network (col.2, lines 35-36). Kaler's invention analyzes data performance (col.12, lines 20-60) and to reduce network traffic for events across the network (col.13, lines 30-36). Freund's and Kaler's invention does not necessarily have to have the same exact systems but should perform similar functions and processes for their systems. Further, applicant did not claim specifically what the system entails but claims methods to perform certain functions such as filtering rules for evaluating intrusions. Thus, applicant's invention includes analyzing the performance for security purposes of preventing intrusions. Both prior art teaches filtering process of data and its traffic, thus is the proper combination.

Freund discloses access rules for workstations which include lists of applications or versions that can be used in order to access which is the active networked application. Further, Freund discusses monitoring and filtering work that is responsible for intercepting process loading and unloading (col.4, lines 5-33 and col.5, lines 55-62). Therefore, Freund does have the claimed filtering rules corresponding to the active networked application (col.10, lines 17-67). The claimed set of intrusion rules is merely interpreted as more than one intrusion rules where Freund does teach more than one intrusion rules and subset rules for the client computer (col.5, lines 35-62). Freund not only discloses monitoring and filtering rules for the user but the client computer. Monitoring the application of the computer being used is to access the internet where there involves rules and subset rules to regulate access on a per application basis (col.10). These filtering rules and subset rules, which includes monitoring a given active application, total time particular applications access the Internet, and limiting the number of (approved) applications are security measures for evaluating the active networked applications for intrusions. The set of intrusion rules includes criterias which now is the subset of rules. The subset rules is inherently the process of reduction to further simplify or to narrow the scope of criterias. Freund does teach filtering rules and subset of rules for applications accessing the Internet as discussed earlier.

Freund did discuss subset rules but not explain in details the process of subset rules, therefore, Kaler was brought forth to explain the filtering creating subset rules process. Kaler discloses that a filter is a way in which a user can specify what is to be monitored in the system under examination (col.22, lines 2-7) wherein includes monitoring applications that performs filter reduction.

Claim 51 included new subject matter that was not originally claimed nor in the specification. The proposed claim stated "a new connection never previously made" is interpreted as a brand new connection that never made or completed attempts before. Whereas, the specification states "a new, previously unseen connection", is not the same as a new connection "never" previously made. The claimed previously unseen connection of the specification is interpreted as a connection that was previously undetected or unknown of but does not mean a connection that was never made. Therefore, claim 51 remains rejected as disclosing new subject matter. All other claims are rejected due their related independent claims being rejected as discussed above. .



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100